

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-273259

(43)Date of publication of application : 05.10.2001

(51)Int.Cl. G06F 15/00  
G06F 13/00

(21)Application number : 2000-088947

(71)Applicant : MITSUBISHI ELECTRIC SYSTEMWARE CORP

(22)Date of filing : 28.03.2000

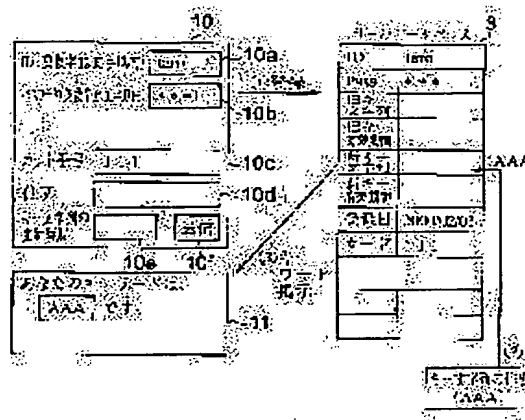
(72)Inventor : ARAKI MICHIKO

(54) SYSTEM AND METHOD FOR USER AUTHENTICATION AND RECORDING MEDIUM RECORDED WITH PROGRAM FOR PERFORMING USER AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To improve security by performing user authentication while using a user ID and a password which are designated by a user and a key character string designated by an authentication system and previously reported to the user.

SOLUTION: When user information required for user registration is inputted to a display picture 10 on a user terminal, a server receives that information, registers that information in a data base 3, prepares a key character string and displays it on the display picture 11 on the user terminal. The user performs log-in while using the key character string reporting like this together with the user ID and the password. The key character string is periodically changed by the server for improving a security effect.



## LEGAL STATUS

[Date of request for examination] 17.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-273259

(P 2 0 0 1 - 2 7 3 2 5 9 A)

(43) 公開日 平成13年10月5日 (2001.10.5)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)		
G06F 15/00	330	G06F 15/00	330	E	5B085
13/00	354	13/00	354	Z	5B089

審査請求 未請求 請求項の数19 O L (全18頁)

(21) 出願番号 特願2000-88947 (P 2000-88947)

(22) 出願日 平成12年3月28日 (2000.3.28)

(71) 出願人 394013002

三菱電機システムウェア株式会社

神奈川県横浜市戸塚区川上町87番地 1

(72) 発明者 荒木 美千子

神奈川県横浜市戸塚区川上町87番地 1 三

菱電機システムウェア株式会社内

(74) 代理人 100057874

弁理士 曾我 道照 (外6名)

F ターム (参考) 5B085 AA08 AC04 AE02 AE23 BG07  
CA04

5B089 GA11 GA21 GB04 HA10 JA31

KA17 KB13 KC58 LB04 LB07

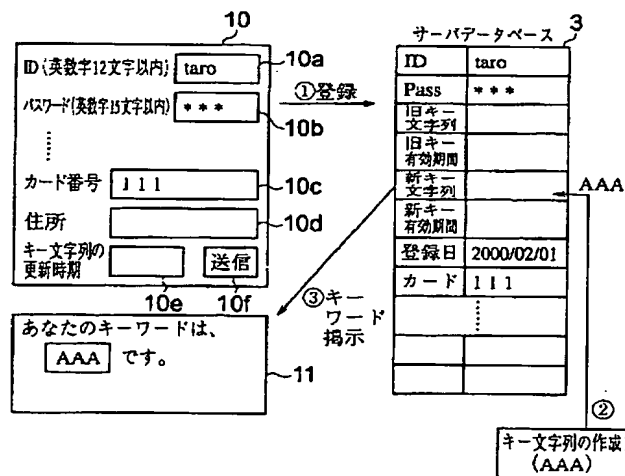
LB14

(54) 【発明の名称】 ユーザ認証システム、ユーザ認証方法およびユーザ認証を行うためのプログラムを記録した記録媒体

(57) 【要約】

【課題】 ユーザにより指定されるユーザID及びパスワードと認証システムにより指定され、ユーザに事前に通知されているキー文字列とを用いてユーザ認証を行い、安全性を向上させる。

【解決手段】 ユーザ端末の表示画面10に対してユーザ登録に必要なユーザ情報を入力すると、サーバがそれを受け取り、データベース3内にそれらの情報を登録するとともに、キー文字列を作成して、ユーザ端末の表示画面11に表示する。ユーザは、このようにして通知されたキー文字列をユーザID及びパスワードとともに用いてログインを行う。キー文字列は、セキュリティ効果を向上させるため、定期的にサーバにより変更される。



## 【特許請求の範囲】

【請求項 1】 登録されるユーザを識別するための固有識別情報を入力するための入力手段と、

上記ユーザを上記固有識別情報に基づいて管理するユーザ管理記憶手段と、

上記ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、上記ユーザ管理記憶手段に登録する認証システム指定特定情報登録手段と、登録された上記認証システム指定特定情報を上記ユーザに通知する通知手段と、

登録されている上記認証システム指定特定情報を変更もしくは無効にするように上記認証システム指定特定情報登録手段に所定の時間間隔において指示を出力するとともに、上記指示が変更を指示するものであった場合に上記認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力手段と、

上記ユーザからアクセスが行われた場合に、上記ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報を上記ユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、上記ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報を上記ユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合手段と、  
上記照合手段による照合のいずれにおいても一致が確認された場合に、上記ユーザに対して使用許可を与える使用許可手段とを備えたことを特徴とするユーザ認証システム。

【請求項 2】 上記ユーザを特定するための情報の入力を上記ユーザから受けて、当該情報をユーザ指定特定情報として、上記ユーザ管理記憶手段に登録するユーザ指定特定情報登録手段をさらに備え、  
上記照合手段が、上記照合に加えて、さらに、上記ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報を上記ユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定することを特徴とする請求項 1 記載のユーザ認証システム。

【請求項 3】 上記通知手段が、上記認証システム指定特定情報を上記ユーザからの上記固有識別情報の入力があった画面上に表示することにより、上記ユーザに通知することを特徴とする請求項 1 または 2 に記載のユーザ認証システム。

【請求項 4】 上記通知手段が、上記認証システム指定特定情報を電子メールにより上記ユーザに通知することを特徴とする請求項 1 または 2 に記載のユーザ認証システム。

【請求項 5】 上記通知手段が、上記認証システム指定特定情報を F A X により上記ユーザに通知することを特

徴とする請求項 1 または 2 に記載のユーザ認証システム。

【請求項 6】 上記通知手段が、上記認証システム指定特定情報を所定の郵便物により上記ユーザに通知することを特徴とする請求項 1 または 2 に記載のユーザ認証システム。

【請求項 7】 上記通知手段が、上記認証システム指定特定情報を暗号化して上記ユーザに送信することを特徴とする請求項 1 ～ 4 のいずれかに記載のユーザ認証システム。

【請求項 8】 課金・請求処理を行うための課金処理手段をさらに備えたことを特徴とする請求項 1 ～ 7 のいずれかに記載のユーザ認証システム。

【請求項 9】 上記認証システム指定特定情報の上記有効期間に対して課金・請求処理を行うための課金処理手段をさらに備えたことを特徴とする請求項 1 ～ 7 のいずれかに記載のユーザ認証システム。

【請求項 1 0】 登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、

上記ユーザを上記固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、

上記ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、上記データベースに登録する認証システム指定特定情報登録ステップと、登録された上記認証システム指定特定情報を上記ユーザに通知する通知ステップと、

登録されている上記認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、上記指示が変更を指示するものであった場合に上記認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、

上記指示に基づいて、上記データベースに登録されている上記認証システム指定特定情報を変更または無効にして上記データベースに再登録する認証システム指定特定情報再登録ステップと、

上記ユーザからアクセスが行われた場合に、上記ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報を上記ユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、上記ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報を上記ユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、

上記照合手段による照合のいずれにおいても一致が確認された場合に、上記ユーザに対して使用許可を与える使用許可ステップとを備えたことを特徴とするユーザ認証方法。

【請求項 1 1】 上記ユーザを特定するための情報の入力を上記ユーザから受けて、当該情報をユーザ指定特定

情報として、上記データベースに登録するユーザ指定特定情報登録手段をさらに備え、

上記照合ステップにおいて、上記照合に加えて、さらに、上記ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報を上記ユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定することを特徴とする請求項 1 0 記載のユーザ認証方法。

【請求項 1 2】 上記通知ステップにおいて、上記認証システム指定特定情報を上記ユーザからの上記固有識別情報の入力があった画面上に表示することにより上記ユーザに通知することを特徴とする請求項 1 0 または 1 1 に記載のユーザ認証方法。

【請求項 1 3】 上記通知ステップにおいて、上記認証システム指定特定情報を電子メールにより上記ユーザに通知することを特徴とする請求項 1 0 または 1 1 に記載のユーザ認証方法。

【請求項 1 4】 上記通知ステップにおいて、上記認証システム指定特定情報を F A X により上記ユーザに通知することを特徴とする請求項 1 0 または 1 1 に記載のユーザ認証方法。

【請求項 1 5】 上記通知ステップにおいて、上記認証システム指定特定情報を所定の郵便物により上記ユーザに通知することを特徴とする請求項 1 0 または 1 1 に記載のユーザ認証方法。

【請求項 1 6】 上記通知ステップにおいて、上記認証システム指定特定情報を暗号化して上記ユーザに送信することを特徴とする請求項 1 0 ～ 1 3 のいずれかに記載のユーザ認証方法。

【請求項 1 7】 課金・請求処理を行うための課金処理ステップをさらに備えたことを特徴とする請求項 1 0 ～ 1 6 のいずれかに記載のユーザ認証方法。

【請求項 1 8】 上記認証システム指定特定情報の上記有効期間に対して課金・請求処理を行うための課金処理ステップをさらに備えたことを特徴とする請求項 1 0 ～ 1 6 のいずれかに記載のユーザ認証方法。

【請求項 1 9】 ユーザ認証を行うためのプログラムを記録した記録媒体であって、

登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、

上記ユーザを上記固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、

上記ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、上記データベースに登録する認証システム指定特定情報登録ステップと、

登録された上記認証システム指定特定情報を上記ユーザに通知する通知ステップと、

登録されている上記認証システム指定特定情報を変更もしくはは無効にするように所定の時間間隔において指示を出力するとともに、上記指示が変更を指示するものであ

った場合に上記認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、

上記指示に基づいて、上記データベースに登録されている上記認証システム指定特定情報を変更または無効にして上記データベースに再登録する認証システム指定特定情報再登録ステップと、

上記ユーザからアクセスが行われた場合に、上記ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報を上記ユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、上記ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報を上記ユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、

上記照合手段による照合のいずれにおいても一致が確認された場合に、上記ユーザに対して使用許可を与える使用許可ステップとを備えたことを特徴とするプログラムを記録した記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】 本発明はユーザ認証システム及びユーザ認証方法に関し、特に、パーソナルコンピュータやワークステーション、及び、インターネットに接続されたサーバ等の種々の情報処理装置において、ユーザを特定する特定情報が入力された場合に、その特定情報の入力がユーザ本人によって行われたか否かを認証して、不正アクセスを防止するためのユーザ認証システム、ユーザ認証方法およびユーザ認証を行うためのプログラムを記録した記録媒体に関するものである。

【 0 0 0 2 】

【従来の技術】 従来の一般的なこの種のユーザ認証方法としては、ホストコンピュータやサーバ等の認証システム上に前もって個々のユーザの I D 番号毎にパスワードを登録しておき、使用開始時にユーザ I D とパスワードとをキーボード等の入力装置から入力させて、前もって登録しておいた正規のユーザ I D 及びパスワードとの照合を行い、一致した場合に使用許可を与えるという方法が多く用いられている。

【 0 0 0 3 】 図 1 9 は、このような従来のユーザ認証システムが接続されたネットワークシステムの構成を示した図である。図 1 9 は、インターネットに代表されるネットワークシステムを例に挙げており、図において、1 0 0 は任意の WWW (WorldWide Web) ブラウザと任意の電子メール送受信ソフトウェアを使用するユーザ端末、1 0 1 はインターネット等のネットワーク、1 0 2 a, 1 0 2 b, 1 0 2 c は、ネットワーク 1 0 1 に接続され、個々のホームページを開設している複数のサーバ、1 0 3 a, 1 0 3 b, 1 0 3 c は、各サーバ 1 0 2 a, 1 0 2 b, 1 0 2 c に接続されているデータベース

で、ユーザ ID 毎にパスワードが予め格納されている。

【0004】動作について説明する。ユーザ端末 100 の利用者であるユーザが、例えば、任意の WWW ブラウザを用いて、ネットワーク 101 を介して、サーバ 102 a が開設するホームページの会員となり、ユーザ ID の発行を受け、所定のパスワードの登録をすでに行っているものとする。このとき、ユーザが、ネットワーク 101 を介して、サーバ 102 a のホームページにアクセスすると、サーバ 102 a は、ユーザに対して、ユーザ ID とパスワードの入力を要求する。この要求に対し、ユーザがユーザ ID とパスワードを入力すると、データベース 103 a 内に前もって登録されている正規のユーザ ID 及びパスワードとユーザにより今回入力されたユーザ ID 及びパスワードとの照合が行われ、これらが一致した場合にユーザは使用許可を得ることができ、サーバ 102 a はネットワーク 101 を介してホームページにおける種々のデータをユーザ端末 100 に送信し、それらを表示させる。

【0005】

【発明が解決しようとする課題】従来のユーザ認証方法においては、上述したように、ユーザ ID とパスワードのみでの認証であり、パスワードが第三者に漏れる可能性を考慮して、ユーザが頻繁にパスワードを変更すれば安全性が高まるが、頻繁に変更するためにはユーザの手間がかかるとともに、あまりに頻繁に変更するとユーザの記憶が混乱しパスワードがわからなくなってしまう等の問題が起き、ユーザに要求される負担が大きい、パスワードを減多に変更しないユーザがほとんどであるのが現状である。

【0006】この発明は、かかる問題点を解決するためになされたものであり、認証システム側により定期的に変更されてユーザに通知される所定の文字列を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止するユーザ認証システム、ユーザ認証方法およびユーザ認証を行うためのプログラムを記録した記録媒体を得ることを目的とする。

【0007】

【課題を解決するための手段】この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力手段と、ユーザを固有識別情報に基づいて管理するユーザ管理記憶手段と、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、ユーザ管理記憶手段に登録する認証システム指定特定情報登録手段と、登録された認証システム指定特定情報をユーザに通知する通知手段と、登録されている認証システム指定特定情報を変更もしくは無効にするように認証システム指定特定情報登録手段に所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力手段と、ユーザからアク

セスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合手段と、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可手段とを備えたユーザ認証システムである。

【0008】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、ユーザ管理記憶手段に登録するユーザ指定特定情報登録手段をさらに備え、照合手段が、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定する。

【0009】また、通知手段が、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知する。

【0010】また、通知手段が、認証システム指定特定情報を電子メールによりユーザに通知する。

【0011】また、通知手段が、認証システム指定特定情報を FAX によりユーザに通知する。

【0012】また、通知手段が、認証システム指定特定情報を所定の郵便物によりユーザに通知する。

【0013】また、通知手段が、認証システム指定特定情報を暗号化してユーザに送信する。

【0014】また、課金・請求処理を行うための課金処理手段をさらに備えている。

【0015】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理手段をさらに備えている。

【0016】また、この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム

指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するかどうかを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するかどうかを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたユーザ認証方法である。

【0017】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、データベースに登録するユーザ指定特定情報登録手段をさらに備え、照合ステップにおいて、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するかどうかを判定する。

【0018】また、通知ステップにおいて、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知する。

【0019】また、通知ステップにおいて、認証システム指定特定情報を電子メールによりユーザに通知する。

【0020】また、通知ステップにおいて、認証システム指定特定情報をFAXによりユーザに通知する。

【0021】また、通知ステップにおいて、認証システム指定特定情報を所定の郵便物によりユーザに通知する。

【0022】また、通知ステップにおいて、認証システム指定特定情報を暗号化してユーザに送信する。

【0023】また、課金・請求処理を行うための課金処理ステップをさらに備えている。

【0024】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理ステップをさらに備えている。

【0025】また、この発明は、ユーザ認証を行うためのプログラムを記録した記録媒体であって、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を

行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するかどうかを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するかどうかを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたプログラムを記録した記録媒体である。

【0026】

【発明の実施の形態】実施の形態1. 図1は、本発明におけるユーザ認証システムの構成を示した概略構成図である。図1において、1は任意のWWWブラウザと任意の電子メール送受信ソフトウェアとを使用するユーザ端末、2は、インターネット等のネットワーク101に接続され、登録制のホームページを開設しているサーバであり、3は、サーバ2に接続され、登録されたユーザをユーザID（固有識別情報）に基づいて管理記憶するデータベースで、ユーザID毎にパスワードと後述するキーワードを含むユーザ情報を格納している。なお、本実施の形態においては、サーバ2とデータベース3とがユーザ認証システムを構成している。

【0027】次に、サーバ2の内部構成について説明する。2aは、ユーザ端末1との間のデータの入出力を制御するユーザインターフェース手段、2bは、ユーザを特定するためのパスワードの入力をユーザから受けて、当該パスワードをユーザ指定特定情報として、データベース3に登録するユーザ指定特定情報登録手段、2cは、ユーザを特定するためのキーワードを発行し、当該キーワードを認証システム指定特定情報として、データベース3に登録する認証システム指定特定情報登録手段、2dは、登録されたキーワードをユーザに通知する通知手段、2eは、登録されているキーワードを変更もしくは無効にするための再登録を行うように認証システム指定特定情報登録手段2cに所定の時間間隔において指示を出力する変更／無効指示出力手段である。また、2fは、ユーザからアクセスが行われた場合に、ユーザからユーザIDの入力を受け付けて、入力されたユーザIDをデータベースに登録されているユーザIDと照合し、一致するかどうかを判定する第一の照合手段、2gは、第一の照合手段2fにより一致が確認された場合に、ユーザからパスワードの入力を受け付けて、入力されたパスワードをデータベース3に登録されているパスワードと照合し、一致するかどうかを判定する第二の照合

手段、2 h は、第二の照合手段 2 g により一致が確認された場合に、ユーザからキー文字列の入力を受け付けて、入力されたキー文字列をデータベース 3 に登録されているキー文字列と照合し、一致するか否かを判定する第三の照合手段である。また、2 j はホームページ等の動作のためのメインプログラムが格納されているメインプログラム格納手段で、2 i は、当該メインプログラムによりサーバ 2 の内部動作の制御を行う制御手段であり、上述の第三の照合手段 2 h により一致が確認された場合に、ユーザに対して使用許可を与える動作も行うものである。また、2 k は、データベース 3 との間のデータの入出力を制御するデータベースインターフェース手段である。

【0028】動作について説明する。図 2 は、サーバ 2 のホームページにユーザ登録を行うための処理の流れを示したフローチャートであり、図 3 は、その動作を説明するための説明図である。図 3 において、10 はユーザ登録を行うためのユーザ端末 1 における表示画面、11 はユーザ登録後のユーザ端末 1 の表示画面である。表示画面 10 には、図のように、ユーザ ID、パスワード、カード番号、住所等のユーザ情報の入力を行うための入力欄 10 a ~ 10 d が設けられている。また、図 3 に、サーバ 2 に接続されているデータベース 3 の一例が示されており、データベース 3 には、図のように、ユーザ ID、パスワード、旧キー文字列、旧キー文字列の有効期間、新キー文字列、新キー文字列の有効期間、登録日、カード番号等が格納されている。

【0029】図 2 のフローチャートに示すように、まず、ステップ S 1 において、サーバ 2 が開設するホームページにユーザ登録を行いたいユーザは、任意の WWW ブラウザを用いて、ネットワーク 101 を介して、当該ホームページにアクセスし、ユーザ端末 1 に設けられたキーボード及びマウス等の入力手段（図示せず）により、表示画面 10 の入力欄 10 a ~ 10 d に対して、ユーザ ID、パスワード、カード番号、住所等の項目について入力を行う。入力が終わると、ユーザは、表示画面 10 の「送信」ボタン 10 f をクリックして、データをサーバ 2 に送信する指示をユーザ端末 1 に与える。当該指示により、入力されたデータは、ネットワーク 101 を介して、サーバ 2 に送信され、サーバ 2 は、ユーザインターフェース手段 2 a により当該データを受信すると、制御手段 2 i により、ステップ S 2 において、必要な項目がすべて入力されているか否かを判定し、入力されていた場合には、ステップ S 3 において、入力されたデータが不正な値か否かを判定し、不正でない場合には、ステップ S 4 において、認証システム指定特定情報登録手段 2 c によりキー文字列の作成を行う。ここで、キー文字列とは、サーバ 2 が所定の時間間隔で変更させる文字列で、例えば、数字、アルファベットまたは記号からなる文字列、もしくは、それらの組合せから構成さ

れるものであり、ユーザ ID 及びパスワードとともに、ユーザ認証に用いる特定情報の 1 つである。作成方法としては、乱数等を用いてランダムに発生させてもよく、また、サーバ側のオペレータ等が適当に定めた所定の文字列から構成するようにしてもよい。文字列の長さとしては、4 ケタ ~ 8 ケタ程度が、実用上かつ安全性上適当である。次に、ステップ S 5 において、認証システム指定特定情報登録手段 2 c が、ステップ S 4 で作成したキー文字列（図 3 の例では「AAA」とする）、ユーザ ID、パスワード等をデータベース 3 に登録する。次に、通知手段 2 d により、ステップ S 6 において、ユーザ端末 1 にネットワーク 101 を介して当該キー文字列を送信し、図 3 に示すように、ユーザ端末 1 の表示画面 11 に、例えば、「あなたのキーワードは AAA です。」のようにキー文字列を表示してユーザに掲示する。以上でユーザ登録は完了するので、ステップ S 7 の所望のメイン処理に移行する。なお、上述のステップ S 2 または S 3 において、ユーザによって入力されたデータが適切でないと判定された場合には、ステップ S 8 において、登録不成功のメッセージがユーザ端末 1 の表示画面に表示される。

【0030】ここで、キー文字列は、上述したように、サーバ 2 により所定の時間間隔で変更されるものであり、従って、所定の期限内で有効であり、期限が経過すると、その時点で無効となる。この期限は原則としてサーバ側で予め定めた所定の期間とするが、複数の期限の候補を用意しておき、すなわち、1 ケ月、2 ケ月、3 ケ月というように用意しておいて、それをユーザが選択できるようにしてもよい。また、ユーザ側がキー文字列の更新時期を指定できるようにしてもよい。ユーザが選択または指定する場合には、上述の図 3 の表示画面 10 の入力欄 10 e を用いて、キー文字列の更新時期を入力するようにすればよい。

【0031】図 4 は、キー文字列の有効期限内にユーザがログインする場合の処理の流れを示したフローチャートである。また、図 5 は、その動作を説明するための説明図である。図 5 において、12 はログインを行うためのユーザ端末 1 における表示画面、13 はログイン後のユーザ端末 1 の表示画面である。

【0032】図 4 に示すように、まず、ステップ S 11 において、ログインを行いたいユーザは、ユーザ端末 1 に設けられたキーボード及びマウス等の入力手段（図示せず）を用いて、表示画面 12 の入力欄 10 g に対して、ユーザ ID の入力を行う。入力されたユーザ ID は、ネットワーク 101 を介して、サーバ 2 に送信される。サーバ 2 は、当該データを受信すると、ステップ S 12 において、第一の照合手段 2 f により、データベース 3 内のデータを検索して、入力されたユーザ ID が登録されているか否かを判定し、入力されていた場合には、ステップ S 13 において、入力されたユーザ ID が

使用可能のものか否かを判定する。使用可能であった場合には、ステップ S 14 において、表示画面 12 の入力欄 10 h にパスワードの入力を行うようにユーザに促す。ユーザがそれに従い、パスワードを入力すると、サーバ 2 がそれを受信する。次に、ステップ S 15 において、第二の照合手段 2 g により、入力されたパスワードとデータベース 3 内に予め登録されている正規のパスワードとの照合を行い、パスワードが一致していた場合には、次に、ステップ S 16 において、表示画面 12 の入力欄 10 i にキー文字列の入力を行うようにユーザに促す。ユーザがそれに従い、キー文字列を入力すると、サーバ 2 がそれを受信し、次に、ステップ S 17 において、第三の照合手段 2 h により、入力されたキー文字列とデータベース 3 内に予め登録されている正規のキー文字列との照合を行い、キー文字列が一致していた場合には、ユーザに使用許可が与えられ、図 5 の表示画面 13 に示されるように、ログイン成功のメッセージが表示される。以上でログイン処理が完了されるので、ステップ S 18 のメイン処理に移行される。なお、上述のステップ S 12、S 13、S 15 または S 17 において、ユーザによって入力されたユーザ ID、パスワード、または、キー文字列が適切でないと判定された場合には、ステップ S 19 において、ログイン不成功のメッセージがユーザ端末 1 の表示画面に表示される。

【0033】次に、キー文字列の有効期限が経過した場合の更新の処理について説明する。前提条件として、本実施の形態においては、キー文字列の有効期限は、ユーザ登録の日付にかかわらず、毎月の 1 日～末日までとする。現時点においては、先のキー文字列の有効期限はすでに経過しており、サーバ 2 の変更／無効指示出力手段 2 e により認証システム指定特定情報登録手段 2 c に指示が出され、先のキー文字列は無効となっているものとする。なお、認証システム指定特定情報登録手段 2 c のキー文字列を無効にする動作としては、データベース 3 内の新キー文字列のデータ領域に格納されているキー文字列をデータベース 3 内の旧キー文字列のデータ領域に移動させるとともに、新しいキー文字列として、例えば“NULL”を発行し、それをデータベース 3 内の新キー文字列のデータ領域に登録するようにすればよい。

【0034】図 6 は、旧キー文字列が無効となった以降に最初にユーザがログインする場合のキー文字列の更新の処理の流れを示したフローチャートであり、図 7 は、その動作を説明するための説明図である。図 6 に示すように、まず、ステップ S 21 において、ログインしたいユーザは、ユーザ端末 1 に設けられたキーボード及びマウス等の入力手段（図示せず）を用いて、図 7 の表示画面 12 の入力欄 10 g～10 i に対して、ユーザ ID、パスワード、キー文字列の入力を行う（この場合のキー文字列は、無効となっている旧キー文字列である。）。入力されたこれらのデータは、ネットワークを介して、

サーバ 2 に送信される。サーバ 2 は、当該データを受信すると、ステップ S 22 において、データベース 3 内のデータを検索して、キー文字列の有効期限を確認し、有効期限が経過していた場合には、データベース 3 内の旧キー文字列に当該データが登録されているか否かを判定し、登録されていた場合には、ステップ S 23 において、図 7 の表示画面 14 の入力欄 10 j (Yes) 及び 10 k (No) に対して、契約を更新するか否かの希望を入力するようにユーザに促す。ユーザがそれに従い、“更新 (Yes)” を選択すると、サーバ 2 がそれを受信し、次に、ステップ S 24 において、キー文字列の作成を行う。キー文字列の作成方法等については、上述と同様であるため、ここでは説明を省略する。次に、ステップ S 25 において、ステップ S 24 で新規に作成したキー文字列（図 7 の例では“ZZZ”とする）をデータベース 3 内の新キー文字列のデータ領域に登録する。次に、ステップ S 26 において、ユーザ端末 1 にネットワークを介して当該キー文字列を送信し、図 7 に示すように、ユーザ端末 1 の表示画面 15 に、例えば、「あなたの今月のキーワードは ZZZ です。」のようにキー文字列を表示してユーザに掲示する。以上でキー文字列の更新処理は完了するので、ステップ S 27 の所望のメイン処理に移行する。なお、上述のステップ S 22 において、ユーザによって入力されたユーザ ID 等が登録されていないと判定された場合、及び、ステップ S 23 において、ユーザが“契約を更新せず (No)” を選択した場合には、ステップ S 28 において、更新不成功のメッセージがユーザ端末 1 の表示画面に表示される。

【0035】以上のように、本実施の形態においては、ユーザ側により登録されるユーザ ID 及びパスワードに加え、サーバ側により定期的に変更されてユーザに通知される所定のキー文字列を用いて、これら 3 種類の情報を組み合わせてユーザ認証を行うようにしたので、安全性が向上する。また、たとえ、ユーザがパスワードを頻繁に変更する作業を怠っていても、サーバ側によりキー文字列は強制的に変更されるので、第三者にユーザ ID、パスワード、キー文字列のすべてが万一漏れた場合にも、次のキー文字列が発行された時点で、これらの漏れた特定情報は無効になるため、第三者の不正アクセスを最小限に食い止めることができる。

【0036】なお、上述の例では、キー文字列の有効期限をユーザ登録の日付にかかわらず、毎月の 1 日～末日までとする例について述べたが、その場合に限らず、本発明はキー文字列をサーバ 2 が強制的に変更することを目的としているため、例えば、ユーザ登録の日から 1 ケ月というように、有効期限の起算日をユーザ登録の日としてもよく、また、1 ケ月ではなく、毎日ないし 1 週間程度で変更するようにしてもよい。

【0037】また、上述の例では、ユーザからの契約更新の指示を受けて、新しいキー文字列を発行する例につ

10

20

30

40

50



いて述べたが、その場合に限らず、有効期限が経過したら、自動的に、変更／無効指示出力手段 2 e の指示により、新しいキー文字列が発行されて、それがデータベース 3 に登録されるとともに、ユーザに通知されるようにしてもよい。

【0038】実施の形態 2. 上述の実施の形態 1 においては、サーバ 2 により作成されたキー文字列を WWW ブラウザによりユーザに対して掲示する方法について述べたが、本実施の形態においては、電子メールによりユーザに対して通知する例について説明する。図 8 は本実施の形態におけるユーザ登録動作の処理の流れを説明するための説明図であり、図 9 はキー文字列の期限経過後の更新動作の処理の流れを説明するための説明図である。これらの図において、4 は、サーバ 2 に接続され、メールの送受信を行うメールサーバであり、図 8 の 10 m 及び 10 n はメールアドレス及びユーザが契約しているプロバイダ名を入力するための入力欄であり、図 8 の 40 及び図 9 の 41 は共にメールサーバ 4 によりユーザに対して配信された電子メールである。他の構成については上述の実施の形態 1 と同一であるため、同一符号を付して示している。なお、本実施の形態における有効期限内のログイン動作については、上述の実施の形態 1 (図 4 及び図 5 参照) と同一であるため、ここでは説明を省略する。

【0039】動作について説明する。まずはじめに、ユーザ登録動作について説明する。処理の流れは、基本的には図 2 のフローチャートと同様であるため、これを参照しながら説明する。まず、ステップ S 1 において、上述の実施の形態 1 で示したユーザ ID 等の項目に加えて、本実施の形態においては、メールアドレス及びユーザが契約しているプロバイダ名を入力する。ステップ S 2 ～ S 5 までの処理は全く同一である。ステップ S 6 において、本実施の形態では、ユーザ登録を行ったユーザに対して、契約してある所定のプロバイダを介して、電子メールを配信し、図 8 に示すように、例えば、「あなたのキーワードは AAA です。」のようにキー文字列を通知する。本実施の形態においては、以上でユーザ登録は完了する (ここでは、図 2 のステップ S 7 のメイン処理の工程はない。)。なお、図 2 のステップ S 2 または S 3 において、ユーザによって入力されたデータが適切でないと判定された場合には、ステップ S 8 において、登録不成功のメッセージをユーザ端末 1 の表示画面に表示させる。

【0040】次に、キー文字列の期限満了後の更新動作について説明する。この処理は、基本的に図 6 のフローチャートと同様であるため、これを参照しながら説明する。ステップ S 21 ～ S 25 までの処理は全く同一である。ステップ S 26 において、本実施の形態においては、契約を更新したユーザに対して、契約してある所定のプロバイダを介して、電子メールを配信し、図 9 に示

すように、例えば、「あなたの今月のキーワードは ZZ Z です。」のようにキー文字列を通知する。本実施の形態においては、以上でキー文字列の更新処理は完了する (ここでは、ステップ S 27 のメイン処理の工程はない。)。なお、図 6 のステップ S 22 において、ユーザによって入力されたユーザ ID 等が登録されていないと判定された場合、及び、ステップ S 23 において、ユーザが「契約を更新せず (No)」をユーザが選択した場合には、ステップ S 28 において、更新不成功のメッセージをユーザ端末 1 の表示画面に表示させる。

【0041】以上のように、本実施の形態においては、上述の実施の形態 1 と同様の効果が得られるとともに、さらに、サーバ 2 が作成したキー文字列を電子メールを介してユーザに通知するようにしたので、ユーザ端末 1 からサーバ 2 にアクセスする経路 (ネットワーク) とは別の経路 (電子メール) でユーザに通知するようにしたので、キー文字列を第三者に盗み取られる危険性をより低減できる効果がある。

【0042】なお、本実施の形態においては、キー文字列をユーザに通知するための媒体として電子メールを用いる例について述べたが、その場合に限らず、例えば、FAX や郵便物により通知するようにしても、同様の効果が得られる。本明細書においては、郵便物として、郵便によるハガキ、手紙等の郵便物全般、電報、及び、宅急便等による配達物をすべて含むものとする。

【0043】実施の形態 3. 上述の実施の形態 1 においては、サーバが作成したキー文字列をネットワークを介して送信し、また、ユーザがログインする時などに、ユーザ端末 1 からサーバ 2 へユーザ ID、パスワード、キー文字列を送信するが、このとき、いずれもネットワークを介して送信するため、第三者にそれらの情報を盗み取られる危険性がある。そのため、本実施の形態においては、これらの情報を送信する際に暗号化して送信する例について説明する。暗号化アルゴリズムは、大きく分けて、共通鍵暗号方式と公開鍵暗号方式の 2 種類の方式がある。

【0044】共通鍵暗号方式の場合について簡単に説明すれば、この方式においては暗号化する鍵と復号化する鍵が同じ鍵であるので、ユーザ端末 1 とサーバ 2 とがお互いに共通鍵を保持しておき、送信する場合に情報をその共通鍵で暗号化して送信し、相手方がそれを受信したら、自分が保持している共通鍵で復号化する。

【0045】また、公開鍵暗号方式について簡単に説明すれば、その代表的なものに RSA 方式があり、暗号化鍵と復号化鍵が異なる方式であるため、2 種類の鍵を作成する必要がある。一方が送り手が保持する鍵で秘密鍵と呼ばれるものであり、他方が相手方に渡しておく鍵で公開鍵と呼ばれるものである。ユーザ端末 1 及びサーバ 2 はお互いに相手の公開鍵を保持しているとする。従って、ユーザ端末 1 は自分の秘密鍵 A とサーバ 2 の公開鍵

Bとを保持し、サーバ2は自分の秘密鍵Bとユーザ端末1の公開鍵Aとを保持している。ユーザ端末1は秘密鍵Aで暗号化して送ることも、公開鍵Bで暗号化して送ることもできる。公開鍵Bで暗号化して送ればサーバ2が有する秘密鍵Bでしか解読できないので、第三者に対する安全性を確保することができる。また、秘密鍵Aで暗号化して送れば、安全性の確保に加えて、秘密鍵Aを保持しているのはユーザ端末1のみであるので、情報の送り手がユーザ端末1であるという認証を同時に行えることができる。サーバ2についても同様である。

【0046】以上のように、本実施の形態においては、上述の実施の形態1の効果に加えて、さらに、ユーザ端末1とサーバ2との間で、パスワードやキー文字列のように第三者に知られたくない情報を暗号化して送るようにしたので、より安全性を確保することができる。

【0047】実施の形態4. 本実施の形態においては、上述の実施の形態1～3の構成に、さらに、課金処理手段を追加した例について説明する。図10は、図3の例に課金処理手段を追加した例を示している。図10において、30は、サーバ2に接続されたデータベース3内に追加された課金情報データ、5はサーバ2内に設けられ、課金・請求処理を行う課金処理手段である。課金情報データ30としては、図のように、請求期間、使用料金、使用料金の請求先、引き落とし口座等の情報が格納されている。

【0048】動作について説明する。ユーザ登録の処理の流れは、基本的には図2のフローチャートと同様であるため、これを参照しながら説明する。まず、ステップS1において、上述の実施の形態1で示したユーザID等の項目に加えて、本実施の形態においては、課金処理に必要な使用料金請求先と引き落とし口座を入力する。ステップS2～S4までの処理は全く同一である。ステップS5において、データベースヘデータを登録する際に、本実施の形態においては、課金処理に必要な情報をデータベース3に格納する処理が追加される。ただし、使用料金の項目の初期値は“0”に自動設定されるものとする。以降のステップS6～S8の処理は図2と同じであるため説明は省略するが、ステップS7のメイン処理において、その都度、使用量に応じて使用料金が課金され、課金テーブル30の使用料金の値にその値が加算される。

【0049】有効期限内のログイン動作及びキー文字列の更新動作については実施の形態1と基本的に同じであるが、それぞれ、メイン処理において、その使用量に応じて使用料金が課金され、上述と同様に加算される。

【0050】課金処理手段5は、常に課金テーブル30内の有効期限をチェックし、有効期限が経過したら、有効期限日までの使用料金の合計値を課金テーブル30から読み出して、口座からの引き落とし処理を行うようにユーザより指定された銀行に通知するか、または、ユー

ザの住所宛に郵送するための請求書を作成する。

【0051】以上のように、本実施の形態においては、課金処理手段5を追加したので、上述の実施の形態1～3の効果に加えて、さらに、ユーザに対して使用料金を自動的に請求することができるので、利便性が向上する。

【0052】実施の形態5. 上述の実施の形態1～4については、キー文字列を単にユーザ認証の安全性を高めるために用いる例について述べたが、以下の実施の形態においては、キー文字列のユーザ認証目的に加えた付加的使用目的について説明する。本実施の形態においては、月単位でプロバイダとの契約を結ぶためにキー文字列を用いる例について説明する。図11はユーザ登録、図12は契約期間内でのログイン、図13は契約更新の動作を説明するための説明図である。

【0053】動作について説明する。図11に示すように、ユーザ登録を行う際に、ユーザIDとパスワード等を入力して、「契約」ボタン16aを押すと、サーバ2から1ヶ月間（例えば2000年1月1日～2000年1月31日）だけ有効なキー文字列が提供される。1月31日まではそのキー文字列を使って、図12に示すようにログインできるが、2月1日からはログインできないようにする。

【0054】2月1日以降にログインしようすると、サーバ2がキー文字列から有効期限が切れていることを検出し、図13の表示画面17に示すように、「キー文字列の期限が切れています。契約を更新しますか？」というメッセージを表示する。ユーザがそれに対して、契約更新(Yes)するか否か(No)を選択する。契約更新を選択した場合には、サーバ2により、新しいキー文字列が作成され、ユーザに対して通知される。

【0055】以上のように、本実施の形態においては、ユーザID、パスワード、キー文字列の3つによりユーザの認証を行って、ユーザに使用許可を与えるようにしたので、安全性が高く、契約していない第三者により不正にアクセスされることが防止できるとともに、さらに、月単位のように所定の日数の単位でキー文字列を変更することにより、所定の日数の単位での契約を入手を介さずに自動的に更新することができるので、プロバイダ側での契約更新の作業効率を向上させることができる。

【0056】実施の形態6. 本実施の形態においては、キー文字列の有効期間に対して課金・請求処理を行う例について説明する。なお、ユーザ登録、キー文字列の有効期間内でのログイン及びキー文字列の更新の動作については、上述の実施の形態1と同じであるため説明を省略する。

【0057】動作について説明する。実施の形態1で述べたように、ユーザ登録を行うと、サーバ2から、所定の有効期間において有効なキー文字列が発行される。本

10

20

30

40

50

実施の形態においては、このキー文字列の有効期間に対して課金・請求処理を行う、すなわち、発行されるキー文字列毎に課金・請求処理を行う。課金・請求処理の方法として、大きく分けて、前払いする方法と後払いする方法とがある。

【0058】前払いする場合について説明する。キー文字列を発行する時点（図2のステップS4または図6のステップS24）で、請求書を発行する。キー文字列の有効期限が経過したら、または、使用料金が前払いした金額を超えたら、ログインできないようにする。図7に示したような方法で、契約更新の希望の有無について問い合わせ、ユーザが契約更新を希望したら、新しいキー文字列を発行し、請求書を発行する。このように、前払いの場合には、個々のキー文字列を発行する時点で請求書を発行する。

【0059】次に、後払いする場合について説明する。有効期限をもって、その間の使用料金を加算していき、有効期限が経過したら、請求書を発行するとともに、そのキー文字列においてはログインできないようにして、ユーザが契約更新を希望したら、新しいキー文字列を発行する。新しいキー文字列においても、同様に、有効期限が経過したら請求書を発行する。

【0060】以上のように、本実施の形態においては、ユーザID、パスワード、キー文字列の3つによりユーザの認証を行って、ユーザに使用許可を与えるようにしたので、安全性が高く、契約していない第三者により不正にアクセスされることが防止できるとともに、さらに、キー文字列毎に課金・請求処理を行うようにしたので、課金・請求管理が容易であるとともに、料金を支払わないユーザに対しては新しいキー文字列の発行を停止するようにすることもでき、料金の回収率を高くすることができる。

【0061】実施の形態7. 本実施の形態においては、インターネット上でアンケートに答えると、期間限定のサービスを受けられるキー文字列が提供されるという例について説明する。図14は、本実施の形態の動作を説明するための図である。図14の表示画面60に示されるような所定のアンケートにユーザが答えたとする。サーバ2はアンケート結果を受信すると、入力項目のチェックを行い、問題がなければ、それをデータベースに登録するとともに、キー文字列を作成して、ユーザに送信する。ユーザ端末1には、図14の表示画面61に示されるように、送信されてきたキー文字列とともにその有効期限が表示される。ユーザが、図14の表示画面62に表示されているような「アンケートにお答えいただいた方には、期間限定の「特別価格」で購入できます。キー文字列を入力して送信ボタンを押して下さい。」というメッセージに従って、キー文字列を入力すると、所定の「特別価格」ページが画面に表示される。

【0062】以上のように、本実施の形態においては、

アンケートに答えた人に対してキー文字列を与え、ユーザID、パスワード、キー文字列の3つによりユーザの認証を行って、「特別価格」のページへのアクセスの許可を与えるようにしたので、安全性が高く、アンケートに答えていない第三者により不正にアクセスされることがなく、情報のセキュリティを守ることができる。また、アンケートに答えることにより、特別なサービスを受けることができるようにし、かつ、キー文字列を用いてサービス提供の期限管理を行うようにしたので、アンケートへの回答率の向上と期限管理処理との両面の効率化を図ることができる。

【0063】実施の形態8. 本実施の形態においては、特定のホームページ（もしくはホームページの特定のグループ会員）に登録したユーザにのみホームページ内の所定のページ（有資格領域）の内容が表示されるようにした例について説明する。図15は、本実施の形態におけるホームページの一例を示したものであり、図において、70は当該ホームページを表示している表示画面、71は一般の人が参照できるフリー領域であり、72はユーザ登録したユーザのみが参照できる有資格領域である。一般の人がアクセスすると、フリー領域71のみが表示画面70に表示される。一方、ユーザ登録したユーザがユーザID、パスワード、キー文字列を用いてアクセスすると、図15のように、フリー領域71及び有資格領域72の両方が表示画面70に表示される。

【0064】なお、ユーザの登録動作については、上述の実施の形態1で説明した図2のフローチャートに示す処理に従い、ログインの動作は図4に、キー文字列更新の動作は図6に従うものとする。

【0065】また、上述においては、登録してあるユーザがユーザID、パスワード、キー文字列の3つを用いてログインする例について示したが、その場合に限らず、ユーザIDとパスワードを用いてログインを行うようにしてもよく、その場合には、まず、図16に示すように、フリー領域71部分だけが表示され、その下に、「掲示板」というボタン73が表示され、ユーザが「掲示板」ボタン73にマウスポインタを当てると、「キー文字列を入力。」というメッセージが表示され、それに従って、ユーザがキー文字列を入力欄74に入力して、送信ボタン75を押すと、図15の有資格領域72に相当するページが表示画面70に表示される。

【0066】以上のように、本実施の形態においても、ユーザID、パスワード、キー文字列の3つによりユーザの認証を行って、ユーザに使用許可を与えるようにしたので、有資格領域に登録していない第三者により不正にアクセスされることがなく、情報のセキュリティを守ることができる。

【0067】実施の形態9. 本実施の形態においては、雑誌や本等の種々の文献の購読ができるホームページを想定して、その購読契約にキー文字列を用いる例につい

て説明する。図 17 は当該ホームページにおけるユーザ登録及び購読契約を行うための表示画面を示したものである。上述の実施の形態 1 と同様の手順でユーザ情報を入力し、次に、文献名が記載されている任意のボタンをクリックして、購読契約を行いたい文献を指定した後に、送信ボタン 82 を押すことにより、購読契約を行いたい文献情報がサーバ 2 に送信される。これを受けて、サーバ 2 は、キー文字列を発行し、ユーザに通知する。すなわち、上述の図 2 の処理と異なる点は、ステップ S1 において、ユーザ情報だけを入力せずに、購読契約を行いたい文献名も入力する点である。それ以外の処理は図 2 と同様である。このようにして、ユーザ登録及び購読契約を行ったユーザは、キー文字列の有効期限内において、図 4 の要領でログインすると、契約してある文献の内容を画面で参照またはダウンロードすることができる。なお、キー文字列の更新については、実施の形態 1 と同様に行う。

【0068】なお、購読契約したい文献は 1 冊に限ることなく、複数冊を指定するようにしてもよい。その場合、各文献に対して、それぞれ、別のキー文字列を与えるようにし、課金・請求処理については、上述の実施の形態 6 で示したように、キー文字列ごとに各有効期間に対して課金・請求処理を行うようにする。

【0069】図 18 は、本実施の形態におけるデータベース 3 の一例を示したものである。各文献の契約に関するデータを図 18 に示すように格納するようにすれば、各文献の契約有効期間や課金の管理を容易に行うことができる。図において、85 は各文献の契約に関するデータからなる契約管理データセット、85 a は購読契約した文献名、85 b は契約をした日付、85 c は当該文献の購読有効期間、85 d は購読有効期間の延べ日数、85 e は購読料金、85 f は各文献に対して発行されたキー文字列である。延べ日数 85 d は、1 ヶ月に満たない購読料金を日割り計算する場合のもので、1 ヶ月単位の契約の場合には“1 M”、“2 M”…というデータが格納される。なお、ここでの購読有効期間 85 c はキー文字列の有効期限と同一のものである。従って、キー文字列の有効期間に、ユーザからのアクセスがあった場合には、サーバ 2 は、各文献に対して、契約管理データセット 85 の内容を参照して、ユーザがアクセス可能か否かを検索するようにする。なお、本実施の形態においては、図 18 のデータベース 3 内の 3 X 部分については不要であるため、削除してもよい（3 X を用いる例について、後述の実施の形態 10 においては説明する。）。

【0070】以上のように、本実施の形態においても、ユーザ ID、パスワード、キー文字列の 3 つによりユーザの認証を行って、ユーザに契約文献へのアクセス許可を与えるようにしたので、購読契約をしていない第三者により不正にアクセスされることがなく、情報のセキュリティを守ることができる。

【0071】実施の形態 10. 上述の実施の形態においては、各文献ごとに異なるキー文字列を発行する例について述べたが、本実施の形態においては、ユーザの利便性を考えて、共通のキー文字列により、契約した文献がすべてアクセスできる例について説明する。

【0072】例えば、最初に所定の文献について契約しておき、その後、別の日に他の所定の文献の契約をしたような場合には、2 回目に契約したときに発行されたキー文字列により、最初に契約した分の文献についてもアクセスできるようにする。すなわち、最新の契約時に発行されたキー文字列を用いることにより、過去に契約した文献がすべて参照できるようにすれば、ユーザが複数のキー文字列を覚えておかななくてすむため、ユーザの負担を軽減することができる。

【0073】なお、共通のキー文字列は、データベース 3 内の 3 X 部分に格納する。このとき、各文献ごとの購読有効期間の管理や、課金・請求処理の管理をサーバ 2 が行うための、上述の実施の形態 9 で示したように、各文献ごとのキー文字列を発行してデータセット 85 内のキー文字列 85 f 内に格納するようにしてもよい。ユーザは共通のキー文字列を用いてアクセスを行い、サーバ 2 はユーザ認証には共通のキー文字列を用い、各文献ごとの購読有効期間の管理や、課金・請求処理の管理には個々のキー文字列 85 f を用いる。

【0074】なお、ここでの購読有効期間 85 c は、共通のキー文字列の有効期限とは独立のものである。従って、この購読有効期間 85 c を管理するための手段（図示省略）をサーバ 2 内に設けて、その手段により、購読有効期間を経過した文献についてはデータベース 3 からデータを削除するとともに、購読料金 85 e のデータを基に請求書を作成してユーザに請求するようにする。このとき、個々の文献ごとに請求書を発行してもかまわないが、利便性を考慮すれば、請求書の発行は毎月 1 回とし、1 つの請求書において複数の文献について請求するようにしてもよい。

【0075】このように、購読有効期間を経過した文献についてはデータベース 3 から削除するようにしたので、共通のキー文字列の有効期間内に、ユーザからのアクセスがあった場合には、サーバ 2 はデータベース 3 の内容を参照して、ユーザがアクセス可能な文献を検索するようにする。

【0076】このようにして、サーバ側においては個々のキー文字列を用いて契約文献の管理を行うようにすれば、発行日の異なる複数の雑誌を契約したような複雑な場合にも、ユーザにおいては 1 つの共通のキー文字列により、それらの文献の購読が可能になる。

【0077】なお、上述の実施の形態 1 ～ 10 においては、ユーザ ID、パスワード、キー文字列の 3 つの情報を組み合わせてユーザの認証を行う例について述べたが、この場合に限らず、本発明の目的は、ユーザが頻繁

にパスワードを変更しないことが多々あるため、サーバ側より強制的に定期的にユーザ認証のための情報を変更して安全性を向上させることであるため、ユーザIDとキー文字列だけを用いてユーザ認証を行うようにしてもよい。

【0078】また、上述の実施の形態1～10においては、ユーザ認証のための照合の順序を、ユーザID、パスワード、キー文字列の順で行う例について述べたが、この場合に限らず、ユーザID、キー文字列、パスワードの順でもよく、キー文字列、ユーザID、パスワードの順で行ってもよい。また、ユーザIDとキー文字列だけをユーザ認証に用いる場合には、キー文字列の照合を先に行うようにしてもよい。

【0079】また、上述の実施の形態1～10においては、ネットワークに接続されたサーバから構成されるユーザ認証システムについて説明したが、本発明はそれに限らず、パーソナルコンピュータやワークステーション等を含む種々の情報処理装置に適用することができる。

【0080】

【発明の効果】この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力手段と、ユーザを固有識別情報に基づいて管理するユーザ管理記憶手段と、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、ユーザ管理記憶手段に登録する認証システム指定特定情報登録手段と、登録された認証システム指定特定情報をユーザに通知する通知手段と、登録されている認証システム指定特定情報を変更もしくは無効にするように認証システム指定特定情報登録手段に所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力手段と、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された上記固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合手段と、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可手段とを備えたユーザ認証システムであるので、認証システム側により所定の時間間隔で変更される認証システム指定特定情報を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止することができる。

【0081】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、ユーザ管理記憶手段に登録するユーザ指定特定情報登録手段をさらに備え、照合手段が、上記照合に加え

て、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定するようにしたので、固有識別情報、認証システム側により所定の時間間隔で変更される認証システム指定特定情報、及び、ユーザ指定特定情報の3つの情報を組み合わせてユーザ認証を行うため、さらに安全性を高め、第三者による不正アクセスを防止することができる。

【0082】また、通知手段が、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知するようにしたので、即座に通知することができる。

【0083】また、通知手段が、認証システム指定特定情報を電子メールによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【0084】また、通知手段が、認証システム指定特定情報をFAXによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【0085】また、通知手段が、認証システム指定特定情報を郵便物によりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【0086】また、通知手段が、認証システム指定特定情報を暗号化してユーザに送信するようにしたので、第三者に特定情報が漏れる可能性を低減することができる。

【0087】また、課金・請求処理を行うための課金処理手段をさらに備えているので、自動的に課金・請求処理が行え、利便性が向上する。

【0088】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理手段をさらに備え、認証システム指定特定情報毎に課金・請求処理を行うようにしたので、課金・請求処理のための管理が容易になり、また、料金を支払わないユーザに対しては次のキー文字列の発行を停止する等の制御も容易になる。

【0089】また、この発明は、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録

されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたユーザ認証方法であるので、認証システム側により所定の時間間隔で変更される認証システム指定特定情報を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止することができる。

【0090】また、ユーザを特定するための情報の入力をユーザから受けて、当該情報をユーザ指定特定情報として、データベースに登録するユーザ指定特定情報登録手段をさらに備え、照合ステップにおいて、上記照合に加えて、さらに、ユーザからのユーザ指定特定情報の入力を受け付けて、入力されたユーザ指定特定情報をユーザ管理記憶手段に登録されているユーザ指定特定情報と照合し、一致するか否かを判定するようにしたので、固有識別情報、認証システム側により所定の時間間隔で変更される認証システム指定特定情報、及び、ユーザ指定特定情報の3つの情報を組み合わせてユーザ認証を行うため、さらに安全性を高め、第三者による不正アクセスを防止することができる。

【0091】また、通知ステップにおいて、認証システム指定特定情報を、ユーザからの固有識別情報の入力があった画面上に表示することによりユーザに通知するようにしたので、即座に通知することができる。

【0092】また、通知ステップにおいて、認証システム指定特定情報を電子メールによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【0093】また、通知ステップにおいて、認証システム指定特定情報をFAXによりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【0094】また、通知ステップにおいて、認証システ

ム指定特定情報を所定の郵便物によりユーザに通知するようにしたので、データのやりとりを行う経路と別の経路を用いてユーザに通知することができるため、第三者に傍受される危険性が低減できる。

【0095】また、通知ステップにおいて、認証システム指定特定情報を暗号化してユーザに送信するようにしたので、第三者に特定情報が漏れる可能性を低減することができる。

【0096】また、課金・請求処理を行うための課金処理ステップをさらに備えているので、自動的に課金・請求処理が行え、利便性が向上する。

【0097】また、認証システム指定特定情報の有効期間に対して課金・請求処理を行うための課金処理ステップをさらに備え、認証システム指定特定情報毎に課金・請求処理を行うようにしたので、課金・請求処理のための管理が容易になり、また、料金を支払わないユーザに対しては次のキーワードの発行を停止する等の制御も容易になる。

【0098】また、この発明は、ユーザ認証を行うためのプログラムを記録した記録媒体であって、登録されるユーザを識別するための固有識別情報を入力するための入力ステップと、ユーザを固有識別情報に基づいてデータベースにより管理するユーザ管理記憶ステップと、ユーザを特定するための情報を発行し、当該情報を認証システム指定特定情報として、データベースに登録する認証システム指定特定情報登録ステップと、登録された認証システム指定特定情報をユーザに通知する通知ステップと、登録されている認証システム指定特定情報を変更もしくは無効にするように所定の時間間隔において指示を出力するとともに、指示が変更を指示するものであった場合に認証システム指定特定情報の有効期間の指定を行う変更／無効指示出力ステップと、指示に基づいて、データベースに登録されている認証システム指定特定情報を変更または無効にしてデータベースに再登録する認証システム指定特定情報再登録ステップと、ユーザからアクセスが行われた場合に、ユーザからの固有識別情報の入力を受け付けて、入力された固有識別情報をユーザ管理記憶手段に登録されている固有識別情報と照合し、一致するか否かを判定するとともに、ユーザからの認証システム指定特定情報の入力を受け付けて、入力された認証システム指定特定情報をユーザ管理記憶手段に登録されている認証システム指定特定情報と照合し、一致するか否かを判定する照合ステップと、照合手段による照合のいずれにおいても一致が確認された場合に、ユーザに対して使用許可を与える使用許可ステップとを備えたプログラムを記録した記録媒体であるので、このプログラムを用いて、認証システム側により所定の時間間隔で変更される認証システム指定特定情報を用いてユーザ認証を行うことにより、安全性を高め、第三者による不正アクセスを防止することができるとともに、プログラム

が記録媒体に記録されているので、種々のシステムに容易に当該プログラムを搭載することができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1におけるユーザ認証システムの構成を示したブロック図である。

【図2】 本発明の実施の形態1におけるユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを示したフローチャートである。

【図3】 図2の動作を説明するための説明図である

【図4】 本発明の実施の形態1におけるユーザ認証システムにおいてキー文字列の有効期限内にログインを行う場合の処理の流れを示したフローチャートである。

【図5】 図4の動作を説明するための説明図である

【図6】 本発明の実施の形態1におけるユーザ認証システムにおいてキー文字列の更新を行う場合の処理の流れを示したフローチャートである。

【図7】 図6の動作を説明するための説明図である

【図8】 本発明の実施の形態2におけるユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを説明するための説明図である。

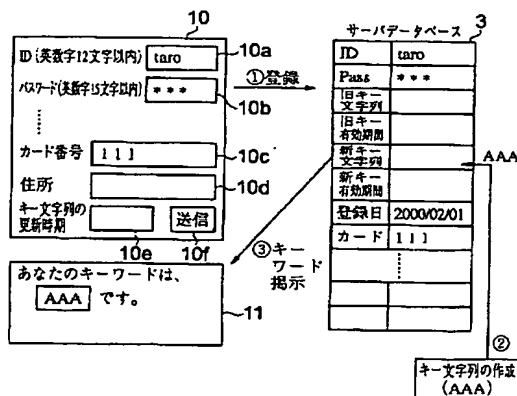
【図9】 本発明の実施の形態2におけるユーザ認証システムにおいてキー文字列の更新を行う場合の処理の流れを説明するための説明図である。

【図10】 本発明の実施の形態4における課金処理手段を加えたユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを説明するための説明図である。

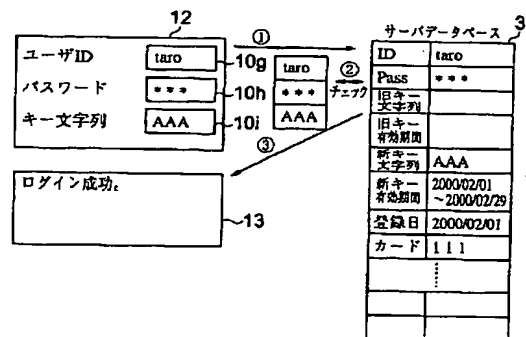
【図11】 本発明の実施の形態5におけるユーザ認証システムにおいてユーザ登録を行う場合の処理の流れを説明するための説明図である。

【図12】 本発明の実施の形態5におけるユーザ認証システムにおいて1ヶ月目のログインを行う場合の処理の流れを説明するための説明図である。

【図3】



【図5】



【図13】 本発明の実施の形態5におけるユーザ認証システムにおいてキー文字列の更新を行う場合の処理の流れを説明するための説明図である。

【図14】 本発明の実施の形態6におけるユーザ認証システムにおいてアンケートへの回答及び特別サービスへのアクセスを行う場合の処理の流れを説明するための説明図である。

【図15】 本発明の実施の形態7におけるユーザ認証システムによるホームページの一例を表示した表示画面を示す図である。

【図16】 本発明の実施の形態7におけるユーザ認証システムによるホームページの他の例を表示した表示画面を示す図である。

【図17】 本発明の実施の形態8におけるユーザ認証システムによるホームページの一例を表示した表示画面を示す図である。

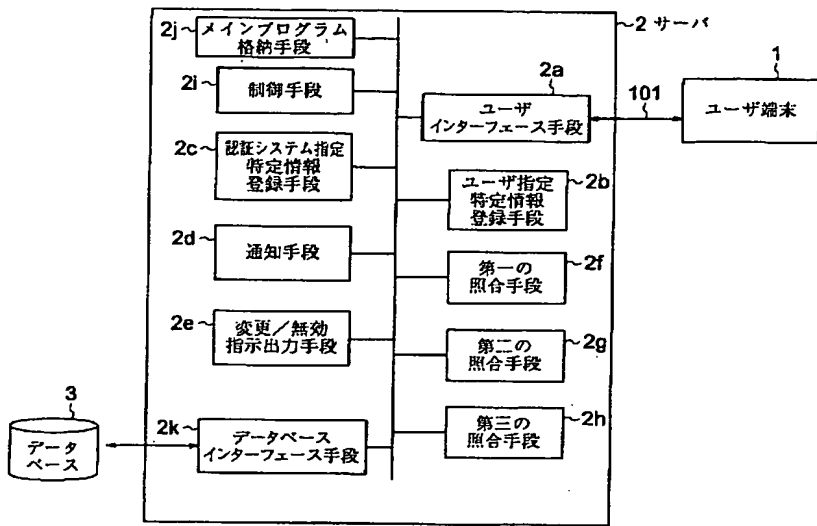
【図18】 本発明の実施の形態8におけるユーザ認証システムにおける購読契約を行った文献を管理するためのデータが追加されたデータベースの一例を示した図である。

【図19】 従来のユーザ認証システムが設けられたネットワークシステム全体を示した概略構成図である。

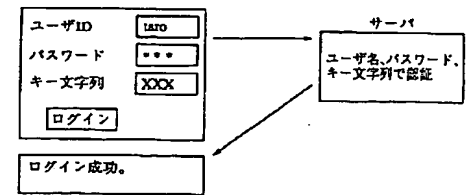
【符号の説明】

1 ユーザ端末、2 サーバ、2 a ユーザインターフェース手段、2 b ユーザ指定特定情報登録手段、2 c 認証システム指定特定情報登録手段、2 d 通知手段、2 e 変更／無効指示出力手段、2 f 第一の照合手段、2 g 第二の照合手段、2 h 第三の照合手段、2 i 制御手段、2 j メインプログラム格納手段、2 k データベースインターフェース手段、3 データベース、4 メールサーバ、5 課金処理手段。

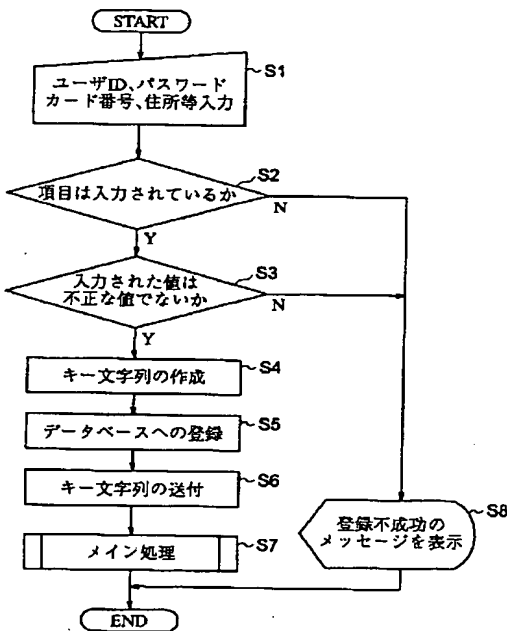
【図1】



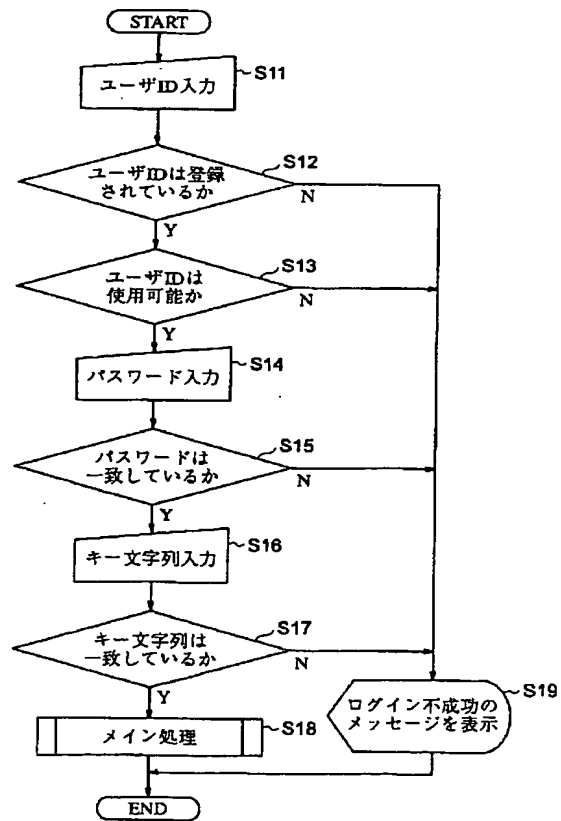
【図12】



【図2】

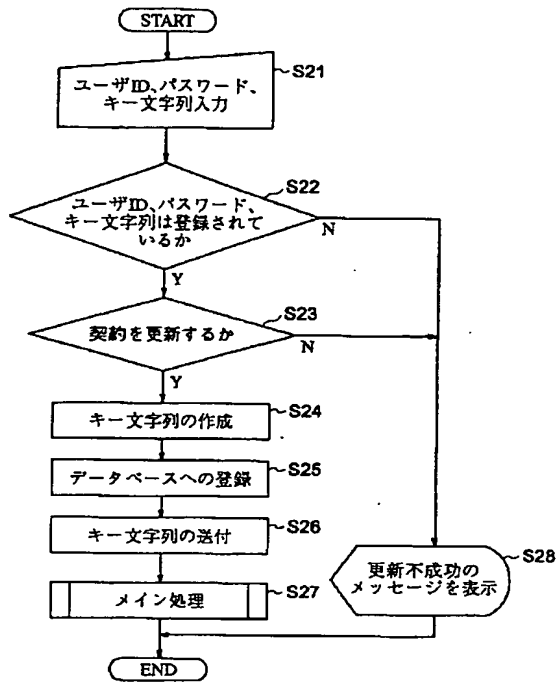


【図4】

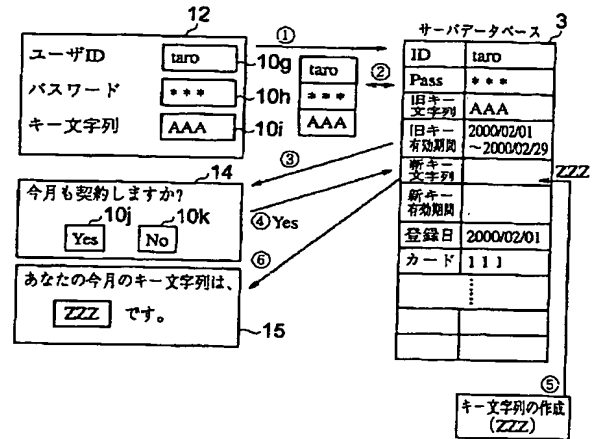




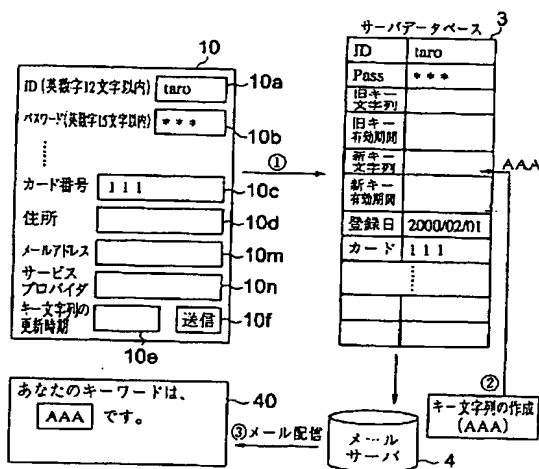
【図6】



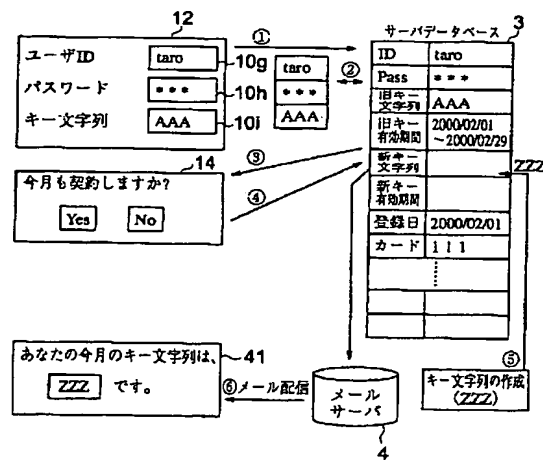
【図7】



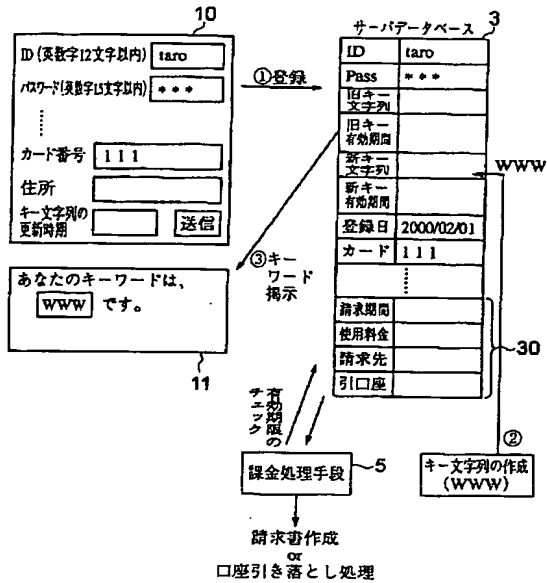
【図8】



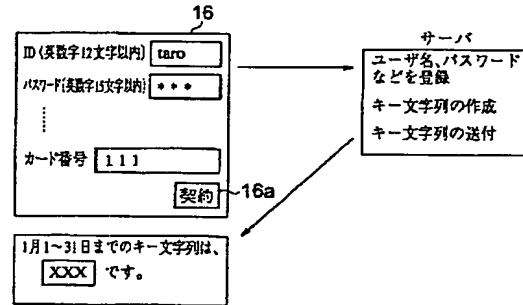
【図9】



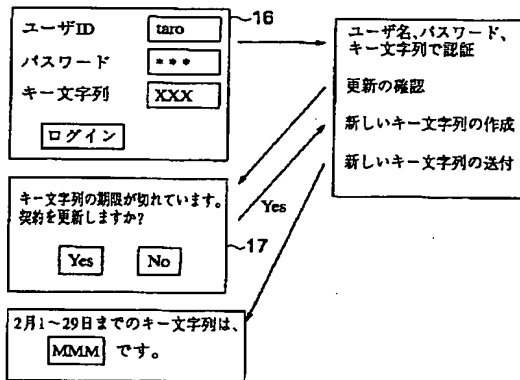
【図 10】



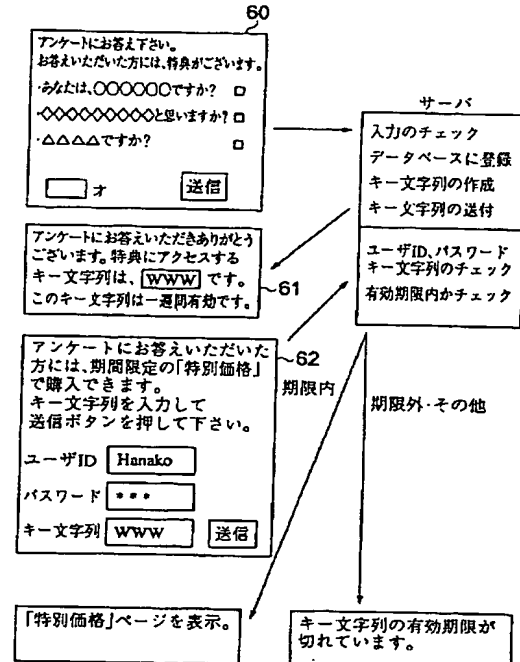
【図 1 1】



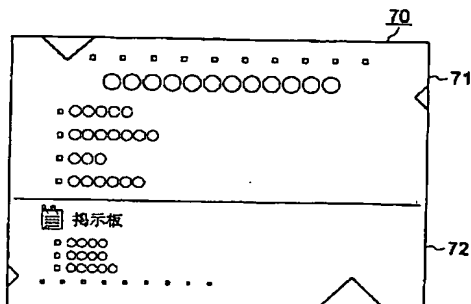
【図 13】



【図 14】



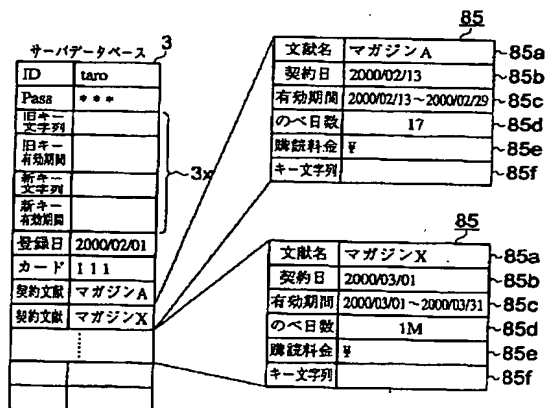
【図 15】



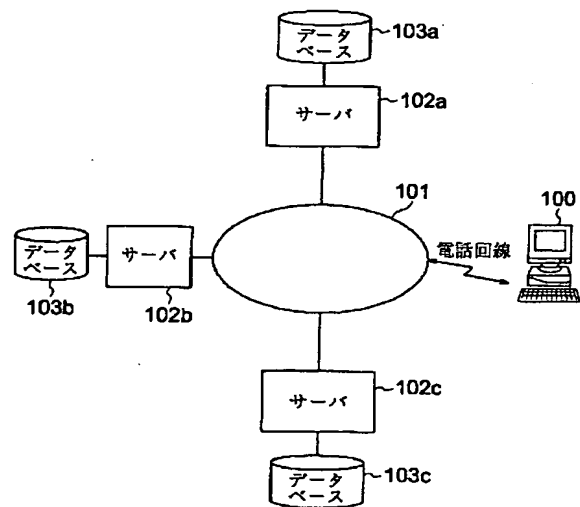
【図16】

【図17】

【図18】



【図19】



101:ネットワーク